E-Authentication

Interim PKI Credential Assessment Profile

12/19/2003
release 1.3.0

Executive Summary

This document is the Credential Assessment Profile for Public Key Infrastructure based credentials. It is part of the Credential Assessment Portfolio as described in the E-Authentication Interim Credential Assessment Framework (CAF). The reader is assumed to be familiar with the CAF. This document contains the specific criteria used to assess PKI based Credential Services (CSs) for use in the E-Authentication initiative.

The Federal government governs PKI based CSs through the Federal Public Key Infrastructure Policy Authority (FPKI PA). The policy mapping determination of the FPKI PA is the basis of this profile. This document specifies the E-Authentication levels that correspond to each of the FPKI PA policy levels.

Release Notes

Interim Release

Document History

Status	Release	Date	Comment	Audience
Release	1.0.0	07/10/03	First Release	Limited
Interim	1.3.0	12/19/03	Released for customer review with the proposal that it be accepted for publication as 2.0.0: • Reduction in tag names for token strength criteria. AND minor proofing amendments which have changed neither the semantics nor the intentions of the document. NB - this document supersedes 1.1.0, which was overtaken by release of the Nov. 2003 draft of NIST SP 800-63 and withdrawn before release.	Customer

Editors

Chris Louden
Kevin Hawkins
Richard G. Wilsher
Dave Silver

David Temoshok
Judy Spencer
Steve Timchak
Von Harrison

Bill Burr
John Cornell
Steven Sill

Table of Contents

1 INTRODUCTION

This document is part of a suite of documents governing the assessment of credentials for use with the E-Authentication Initiative. Please refer to the Interim Credential Assessment Framework (CAF) for an overview.   Additional information can be found at http://www.cio.gov/eauthentication/.   This profile specifies the criteria for Credential Services (CSs) that are based on a Public Key Infrastructure (PKI).

The criteria in this document are primarily based on the findings of the Federal Public Key Infrastructure Policy Authority (FPKI PA).   More information on the FPKI PA is available at http://www.cio.gov/fpkipa/.   A credential service that has not had their policies mapped by the FPKI PA cannot be assessed according to this profile.

2 SCOPE

This profile contains requirements to be met by any Credential Service (CS) based on a PKI.   This document contains the full set of criteria for PKI based CSs, the Common CAP is not applied to PKI systems.

3 TERMINOLOGY

This document relies on terminology and definitions established in the Interim Credential Assessment Framework (CAF).   The most recent version is available at http://www.cio.gov/eauthentication/.   The reader is assumed to be familiar with the Interim CAF.

4 CRITERIA

4.1 Summary

	Level 1	Level 2	Level 3	Level 4
Authentication Protocol	□ Proof of Possession			
Token Strength		□ FPKI Rudimentary	□ FPKI Basic	□ FPKI Medium

4.2 Assurance Level 1

4.2.1 Authentication Protocol

Tag	Description
Proof of possession	The authentication protocol shall prove the claimant has possession and control of the authentication token.

4.3 Assurance Level 2

4.3.1 Token Strength

Tag	Description
FPKI Rudimentary	The FPKI PA must have determined the CS maps to Rudimentary, Citizen and Commerce, or higher.

4.4 Assurance Level 3

4.4.1 Token Strength

Tag	Description
FPKI Basic	The FPKI PA must have determined the CS maps to Basic, Medium, or higher.

4.5 Assurance Level 4

4.5.1 Token Strength

Tag	Description
FPKI Medium	The FPKI PA must have determined the CS maps to Medium or High.